James Arden Barnett, Jr., Rear Admiral (Ret. Navy)

Chief, Public Safety & Homeland Security Bureau

Federal Communications Commission

Press Availability Forum

National Broadband Plan and 700 MHz Proceeding

THURSDAY

February 25, 2010

10:00 a.m.

FCC Headquarters

7th Floor – South Conference Room (7B-516)

Washington, D.C.

INTRODUCTION

Mr. Chairman, thank you. Good morning, we appreciate you joining us. I am pleased to join the Chairman today to highlight major aspects of the FCC's National Broadband Plan and how it relates to public safety and homeland security. Please note that the information that we are sharing on the Plan in advance of its adoption by the Commission and prior to being delivered to Congress is laid out in terms of "working recommendations and potential solutions."

National Wireless Broadband Network for Public Safety

Before I move into various aspects of the Plan, I would like to follow up on the issue highlighted by the Chairman regarding public safety spectrum, and in particular the 700 MHz broadband network. We are committed to moving forward with a framework that will create a nationwide interoperable wireless broadband network for public safety. The National Broadband Plan provides us with a path to move forward, although considerable work will remain for the Commission and the Bureau after the Plan is released.

Police officers and firefighters must be able to talk with each other, share data with emergency managers and transmit critical, time-sensitive information to decision-makers at all levels of government in any type of crisis or emergency situation.

We believe that broadband technologies and innovations will ultimately help us meet this challenge as a nation.

However, the creation of this network is not inevitable. It is essential that the FCC work closely with public safety, our federal, state and local partners and the communications industry to make this a reality.

How do we best meet this challenge?

As the Chairman said, the path forward is dependent on the larger broadband ecosystem that will serve the public, and interoperability must be a core element of public safety broadband from its inception.

We must build on what is already in place and tap into the commercial networks and resources that now exist or are being built.

This will lower costs for public safety, and will enable public safety users to have access to broadband equipment that is affordable and upgradable because it benefits from commercial economies of scale.

The Plan includes a working recommendation that would establish an Emergency Response and Interoperability Center (or ERIC) to assist with network and equipment compatibility, as well as common technical and operating procedures for users of the spectrum. This is a new approach for the Commission, and will draw on resources from other expert agencies such as the U.S. Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST).

By creating ERIC as part of the governing framework for the public safety broadband network from the outset, we seek to avoid the problems we have experienced historically with promoting interoperability in public safety communications.

ERIC will serve as a driving force in the advancement of interoperability standards, authentication, encryption, roaming and priority access, and more for the public safety broadband network. This will be an ongoing role as broadband standards and technology evolve.

The primary goal of ERIC is: to expand public safety's access and use of broadband services nationwide, while ensuring interoperability and operability.

But I want to emphasize that even while our plan envisions partnerships between public safety and commercial entities, and a strong federal regulatory framework focused on ERIC, the recommendations in the Broadband Plan are really about empowering the public safety community to control its broadband destiny rather than relying solely on commercial deployments, and ensuring that its networks meet public safety requirements for hardening, coverage and other characteristics and features.

This is why we have placed such a strong emphasis recommended funding in the Plan.

If we are to create a truly national public safety broadband network, commercial investment alone will be insufficient to ensure resiliency, reliability, and geographic coverage in rural areas, and other public safety standards.

As the Chairman said, funding continues to be the most critical need for public safety.

The Plan may recommend that a grant funding program be established by Congress as a potential solution to provide support for the buildout of the public safety network, as well as its operation and evolution, particularly in rural America.

The details on this are still being worked out, but we are committed to pushing for ideas that will help pay for this network and support its use by public safety.

I'd also like to say a few words about public safety's access to spectrum. The Chairman has explained how the Plan may address D Block, which I know is different from the approach many in public safety have advocated.

We remain committed to the principle that public safety must have access to the spectrum it needs to support broadband applications – and we firmly believe the approach outlined in the Plan is consistent with that principle.

First, public safety will retain its full spectrum allocation in the 700 MHz band, including the 10 MHz that has been licensed to public safety for broadband use. Nothing in the proposed Plan changes this essential fact.

Like any Commission licensee, public safety must abide by FCC rules and technical requirements, but the key point is that this will continue to be public safety's spectrum for their use.

Second, we have devoted much thought in the Plan to how public safety can obtain access not just to the D Block, but to the entire 700 MHz band. This is why we have proposed working recommendations to enable public safety broadband users to roam on commercial networks and obtain priority access on terms that are reasonable and affordable.

Why is this important? Because if public safety has the ability to roam and obtain priority access on commercial networks, it can roam on commercial networks in areas where public safety's own network facilities have not yet been built or are otherwise unavailable. And priority access provides a means for public safety to use additional spectrum capacity in addition to its own dedicated spectrum.

This could be critical in times of emergency, when public safety entities may want to shift non-emergency traffic to other networks in order to reserve their own network and dedicated spectrum for mission-critical communications.

In the long run, though, we recognize that public safety, like all other broadband users, will need access to more spectrum than is available today. This is because demand for high-bandwidth applications will increase, and we also expect that the public safety broadband network will eventually evolve to support mission-critical voice as well as data.

That is why we believe that the proposed working recommendations in the National Broadband Plan, devoted to reclaiming additional spectrum for broadband, are just as important for public safety as they are for commercial broadband providers or the public as a whole.

Reclaiming additional spectrum gives us the long-term option of dedicating some portion of that spectrum for public safety use. But even spectrum that is not dedicated to public safety (and we assume that most reclaimed spectrum would not be) can be accessible and beneficial to public safety.

NBP RECOMMENDATIONS

Now I would like to turn to some of the other key working recommendations that may be included in the National Broadband Plan on public safety and homeland security issues.

Safety and security are vital to America's prosperity and productivity: the ability to prevent emergencies and to respond swiftly when they do occur. Broadband offers transformational promise to public safety and homeland security.

The vision in the Plan will help bring public safety into the broadband world, and will utilize cutting-edge technologies to get us there. There are three major themes associated with the vision, including:

- The ability to respond to all kinds of emergencies through interoperable communications and in seamless coordination with other first responders wherever located throughout the nation; via critical voice and content-rich data to help survivors and save lives.

- Making sure all Americans are able to reach and access emergency services quickly, reliably and with the ability to send and receive critical information regardless of the mode or device used; and

- Revolutionizing the modes and methods by which Americans are alerted and warned of dangers in an accurate, concise and timely way.

In addition to the wireless broadband network, we are looking at other critical areas or gaps in which we believe broadband capabilities and technologies will benefit public safety, including:

- **Critical Infrastructure Protection**: existing policies are inadequate to ensure the cyber security and survivability of our nation's critical infrastructure; and
- **Emergency Communications To and from the Public**: Transition to Next Generation 9-1-1 and emergency alerting is hampered by a lack of intergovernmental coordination, as well as jurisdictional and funding issues that limit the ability of public safety and government agencies to fully transition to broadband and IP-based next generation technologies.

Critical Communications Infrastructure Protection

I'd like to start with cyber security. As the public and private sectors continue to move toward more online usage, there has been a significant increase in cyber attacks. In 2008, the FBI Internet Crime Complaint Center recorded $265 million in reported losses for Internet users.

If cyber security is not addressed, then the transformation to a broadband landscape in America may be hamstrung as consumers may increasingly shy away from entrusting increasing amounts of their personal information and business transactions to a cyberspace that is not secure.

The Commission is taking an active role in working to secure our Nation's vital cyber assets and it is a key focus in the Plan. Accordingly, the Plan may offer a potential solution in which the Commission considers expanding FCC outage reporting requirements currently in place for telecommunications providers to include broadband service providers, including Internet service providers (ISPs).

By increasing our understanding of the genesis and causes of such attacks and how to recover quickly from them, the timely reporting of network outages, including those caused by cyber attacks, by ISPs will help guard against devastating cyber attacks that could cripple broadband communications networks regionally or even globally, and lead to devastating results for our nation's financial institutions and power grid, causing a cascading negative affect on hospital and nursing home care and normal business operations.

As part of these efforts, as you may have heard and/or reported on from my testimony earlier this week before the U.S. Senate Committee on Commerce, Science and Transportation, the Plan includes a working recommendation that the FCC explore the creation of a voluntary cyber security certification process for ISPs that encourages providers to implement enhanced cyber security measures and best practices and other voluntary incentives.

In addition, because a disaster or public health emergency could strike at anytime, there is a potential for broadband networks to quickly become overloaded, slowed or disrupted due to significantly increased use by consumers due to workplace and school closures. To address this, the Plan may recommend the start of an inquiry on the preparedness of commercial networks to withstand network overloads that occur during extraordinary circumstances, such as a bioterrorism event or a pandemic.

This is of particular concern given how usage patterns during a pandemic or bioterrorism event could strain broadband networks. These types of events could undermine network performance for critical users such as first responders and the applications they use.

For example, slowed or disrupted networks could dramatically impede the flow of critical time-sensitive medical and public health information to decision-makers at all levels of government and within the medical community, thereby negatively impacting the public health response.

Information Flow/Prioritizing Broadband Traffic

We also believe that it is absolutely essential that the Commission work closely with the National Communications System, other federal partners and state governments to develop a system of priority network access and traffic routing for first responders and other public safety users on broadband communications networks.

The federal government now has priority communications service programs in place for telecommunications providers for traditional voice communications, including both wireline and wireless services. These programs have proven effective over time to allow first responders, emergency managers and health officials to get their communications through during emergencies. Therefore, we believe it is essential that the Commission work with its federal partners to add broadband communications networks to this emergency preparedness program.

Emergency Communications to and From the Public

Next Generation 9-1-1

I would next like to discuss the Plan's working recommendations for Next Generation 9-1-1 services and how broadband is helping to dramatically change the capabilities of Public Service Answering Points (PSAPs) in many parts of the country. For example, Shelby County, Alabama, just outside of Montgomery, has made the transition to Next Generation 9-1-1 services and is serving as a model for other counties statewide and jurisdictions across the country seeking to incorporate broadband services more fully into their 9-1-1 systems.

However, there continues to be a need to provide increased access to broadband services for the large number of state, county and local 9-1-1 systems that do not have such access. There are a number of reasons why this has occurred, mostly related to the lack of broadband services in many rural areas of the country, and the lack of long-term funding activities that would help localities sustain and further enhance their PSAPs.

To alleviate these roadblocks, the Plan includes a working recommendation that Congress immediately appropriate funding for the National Highway and Traffic Safety Administration to analyze the cost of deploying a Next Generation 9-1-1 system on a nationwide basis. This report should serve as a basis for congressional action to create a coordinated, long-term funding mechanism for the deployment and operation of such a broadband system. Streamlining this process will make the transition to a nationwide Next Generation 9-1-1 system more likely.

Another recommended solution may be for Congress to establish a federal legal and regulatory framework for the development of Next Generation 9-1-1 that removes jurisdictional barriers and inconsistent legacy regulations.

The FCC may, as part of the efforts to implement solutions, consider initiating a proceeding that would address the future roles of 9-1-1 and next generation 9-1-1 as communications technologies, networks and architectures expand beyond traditional voice-centric devices.

Emergency Alerting

Finally, another important area in which we hope the National Broadband Plan will have a significant impact is emergency alerting as it relates to the implementation of the Next Generation Emergency Alert System (or EAS).

The EAS is an important component used to notify the public of sudden emergencies or impending disasters as part of a comprehensive and coordinated emergency response, and we are committed to making the system more reliable and efficient for the benefit of the public and public safety community.

The National Broadband Plan includes a working recommendation in which the Commission would initiate an inquiry this year into the technical, legal and policy issues associated with the development of a multi-platform Next Generation alert system that comprehensively provides for the delivery of alerts at the national, state, tribal and local levels. This will help supplement all of the ways that the public now receives their emergency information, whether it is television or radio broadcast, cable, satellite, wireless devices such as a cell phone or the Internet.

Ultimately, the goal is to help transform the delivery capabilities of EAS during emergencies not only in scope and ability to reach as many people as possible in a variety of ways, but by geographically targeting certain populations, such as persons with disabilities or predominantly non-English speaking communities to receive alerts.

Conclusion

This concludes my briefing on aspects of the National Broadband Plan related to public safety and homeland security. Again, we want to thank you for your time and attention today; and as always we appreciate your coverage. At this time, we will take any questions that you may have.